



Day 2 Kubernetes Beyond the install

Paul Czarkowski
Principal Technologist

@pczarkowski
github.com/paulczar



ELECTRONIC ARTS™

Pivotal™

Pivotal.

bluebox[®]
cloud

IBM[®]

rackspace[®]



A group of people in a workshop setting. A man on the left is pointing at a wall covered in papers. A group of people is seated in the center, and another man is standing on the right. The image has a dark blue overlay.

Who is using Linux Containers ?

A group of people in a workshop setting. A man on the left is pointing at a wall covered in papers. A group of people is sitting on stools in the center, and another man is standing on the right. The image has a dark blue overlay.

Who is using Kubernetes ?

A group of people in a workshop setting. One person is standing and pointing at a wall covered in sticky notes. Several other people are sitting on stools, looking towards the speaker. The scene is dimly lit with a blue tint.

Who is operating Kubernetes ?

A group of people in a workshop setting. A man on the left is pointing at a wall covered in papers. A group of people is seated in the center, and another man is standing on the right. A teal box highlights the seated group.

> 1 year Kubernetes experience?



Successful Kubernetes
deployments are just
as much a cultural challenge
as they are technical.



KubeCon



CloudNativeCon

Europe 2018

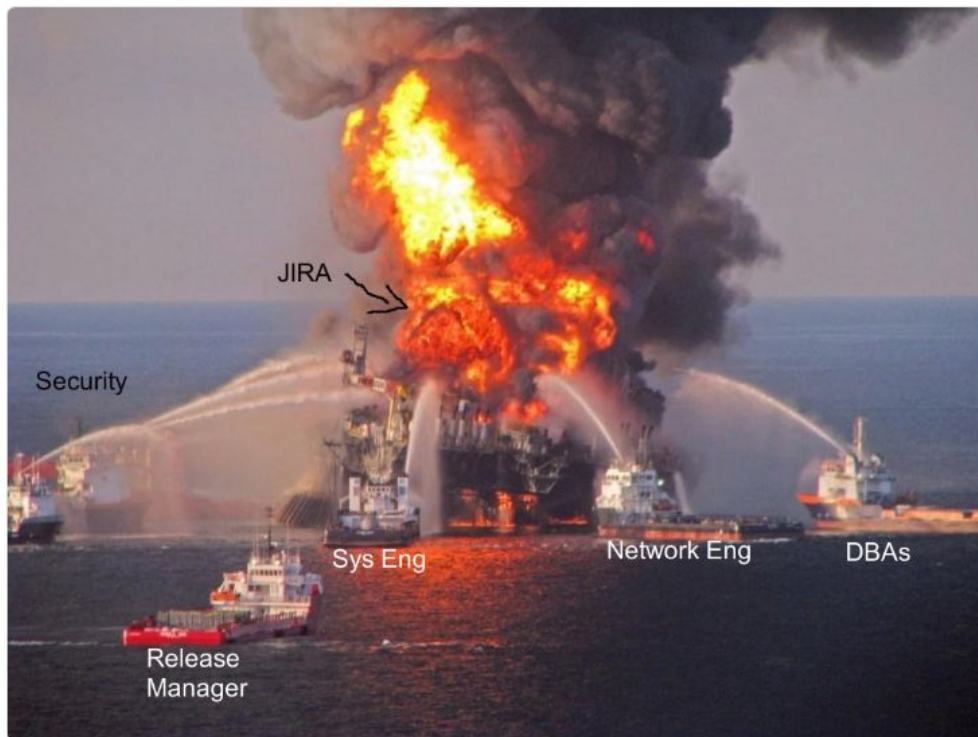


Czarcloudski

@pczarkowski



Enterprise DevOps



11:16 AM - 11 Jun 2018

662 Retweets 1,315 Likes





People build Platforms
People build Apps
Apps run on Platforms

People are the most
important component
of any platform.

A person with glasses and a dark shirt featuring a white geometric logo is seated at a table in a meeting. They are gesturing with their hands while speaking. Two other people are partially visible in the foreground, facing away from the camera. The background is a plain wall.

“Organizations which design systems ... are constrained to produce designs which are copies of the communication structures of these organizations.” - Conways Law



Control loops

Drive **current state** -> **desired state**

Act independently

APIs - **no shortcuts** or back doors

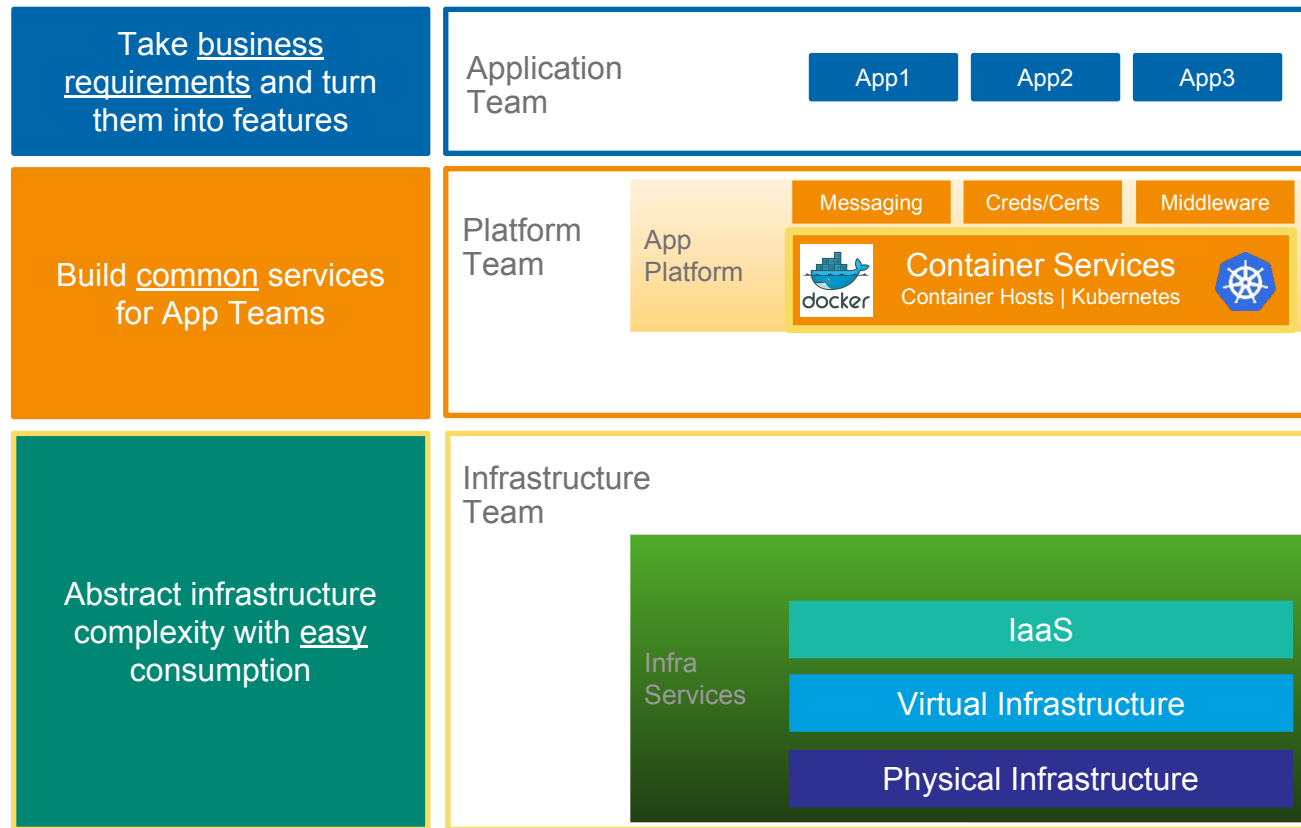
Observed state is truth

Recurring pattern in the system

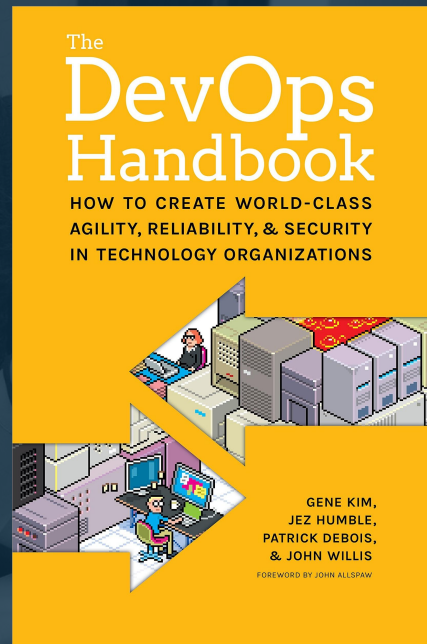
Example: ReplicationController



Evolve your IT teams!



"In general, taking something that's already working somewhere and expanding its usage (capabilities) is far more likely to succeed than building these capabilities from scratch"



Day 1 - Build

Development The team can make progress in developing new features for the platform

CI/CD CI/CD pipelines drive the testing and promotion of artifacts

Consistency Provide a consistent setup experience, across different environment configurations.

Setup time How long does it take to setup a real world working environment? Think hours, not weeks.

Day 2 - Operate & Enhance

Patches Patching App and System components as CVEs occur

Scaling Seamlessly scale platform components to accommodate changing demand.

Upgrades. How do you roll out new versions of the platform with the lights on?

Operating Effort Operating the platform should require very few resources and minimum manual intervention. Otherwise, you will be spending lots on operational support!



Architecture



Czarcloudski

@pczarkowski

Cant tell if london underground map or
openstack architecture diagram.



7:43 AM - 19 Feb 2016

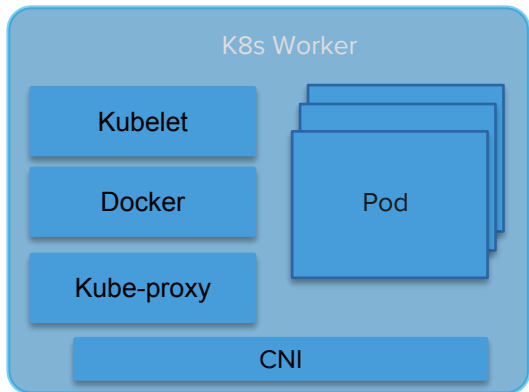
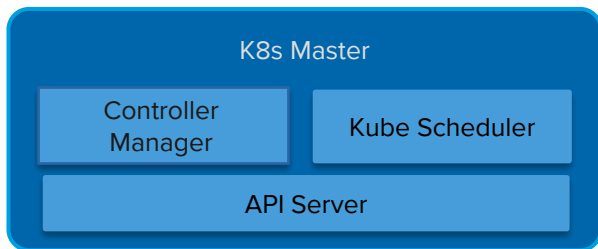
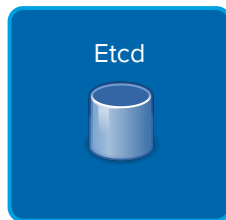
Not like this...

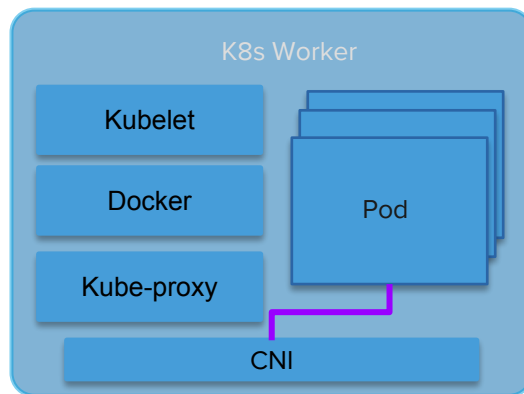
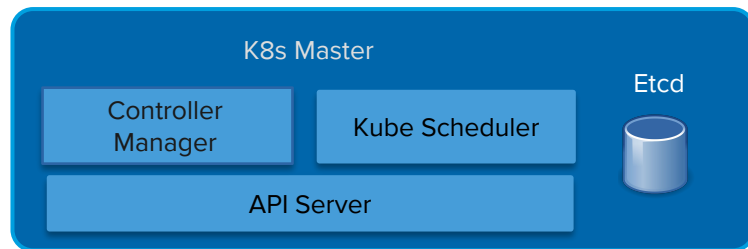


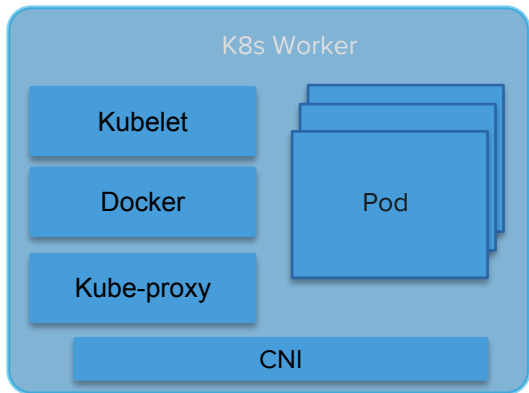
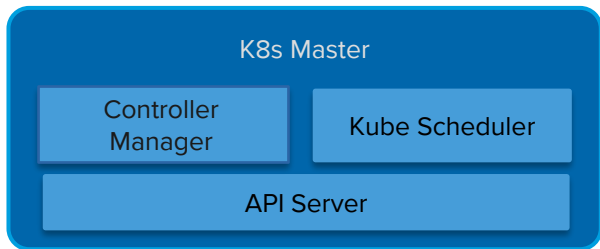
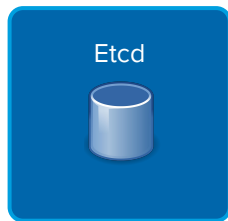
Like this...

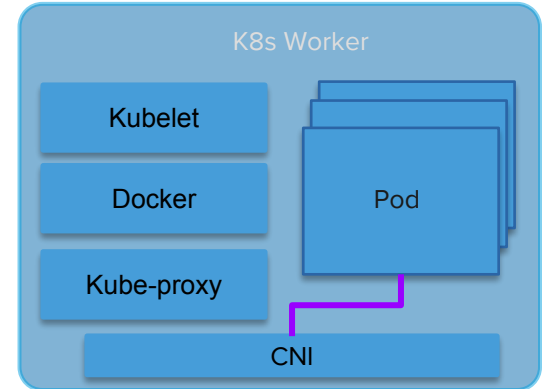
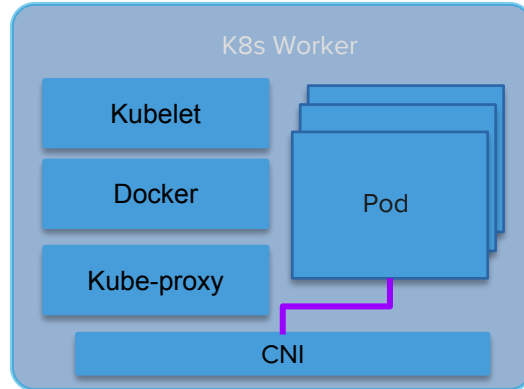
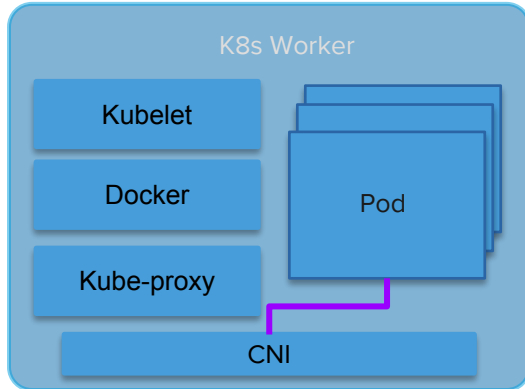
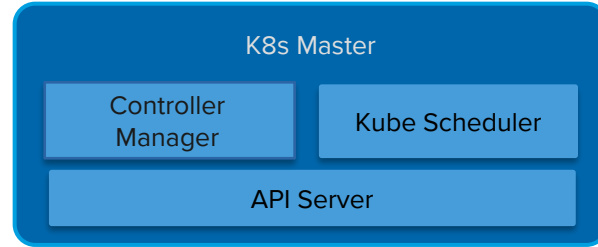
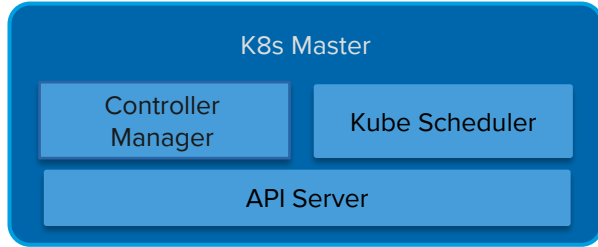
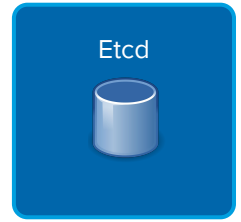


Created by Henrik Kniberg

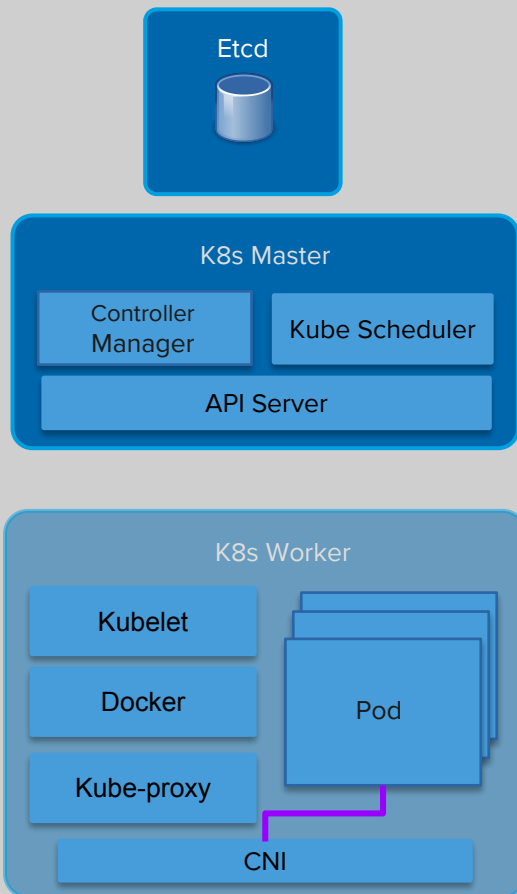




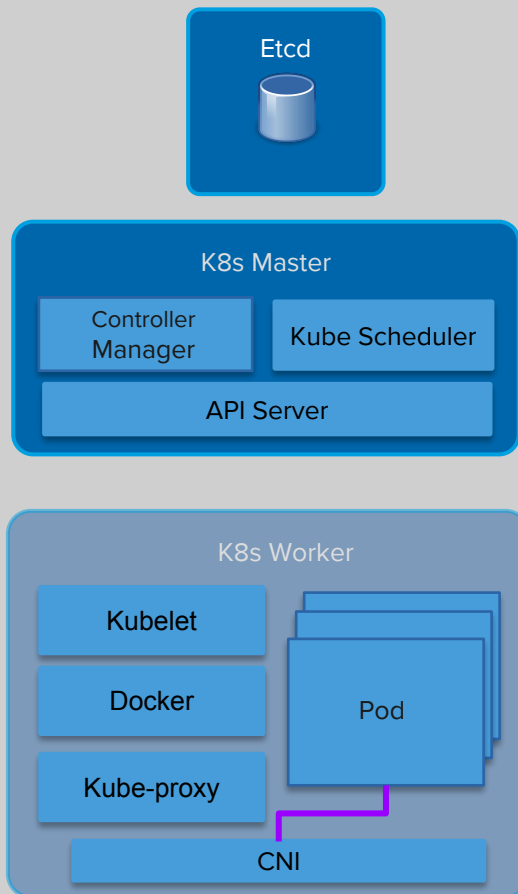




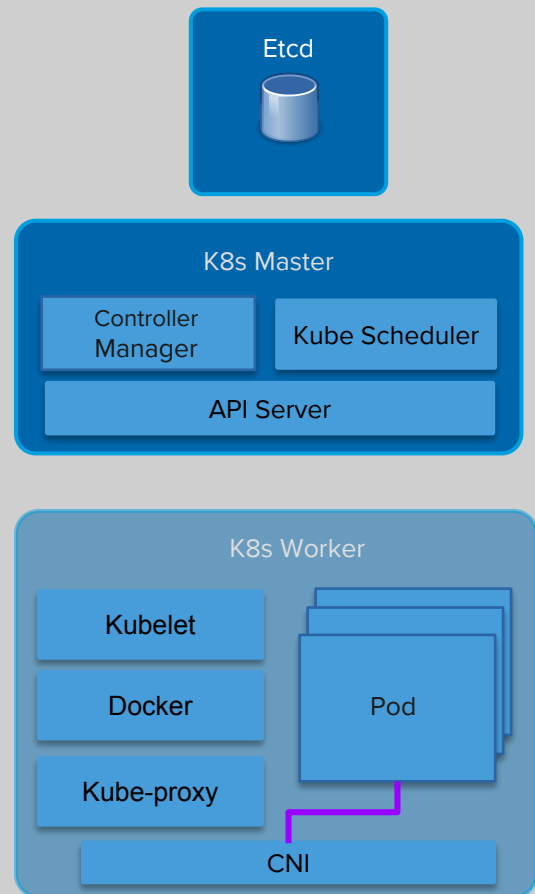
us-tirefire-1a



us-tirefire-1b

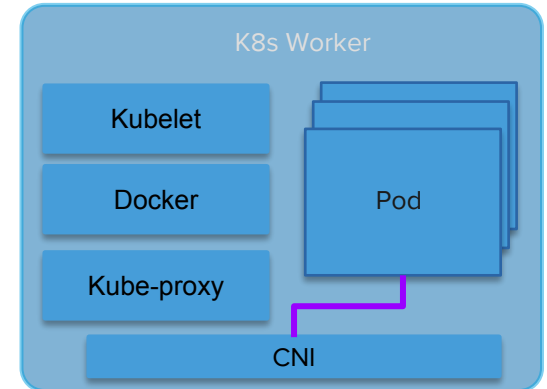
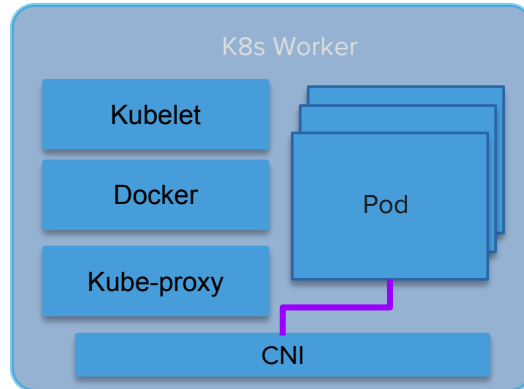
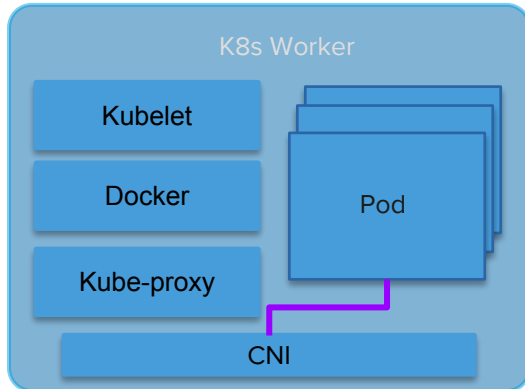
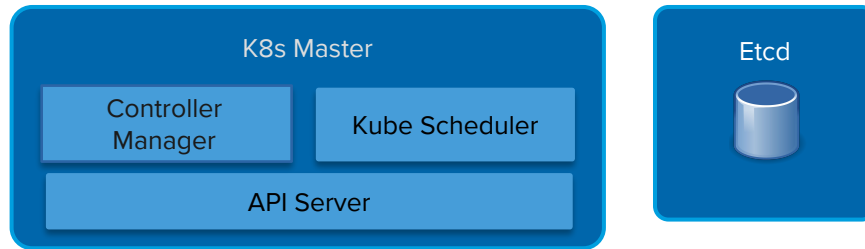


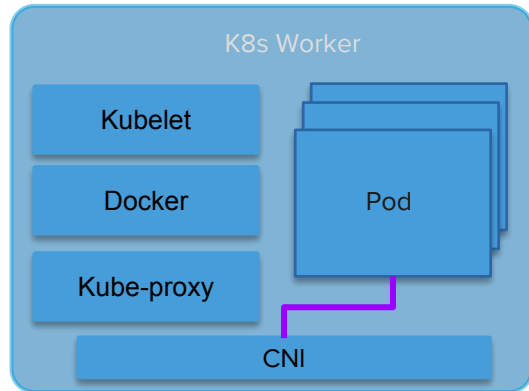
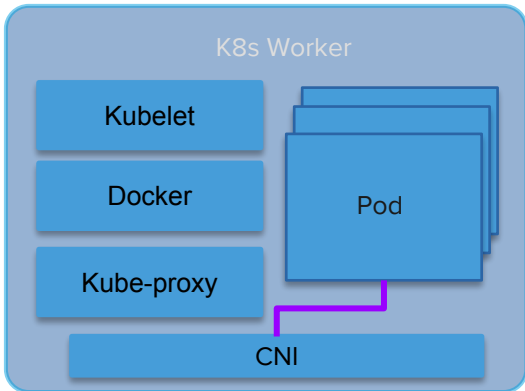
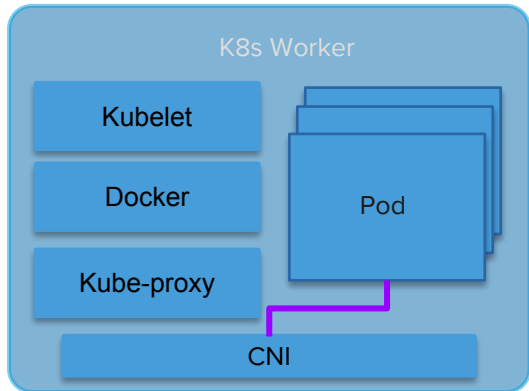
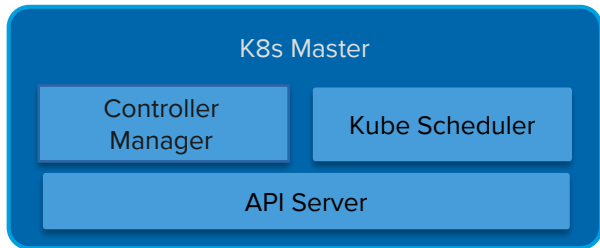
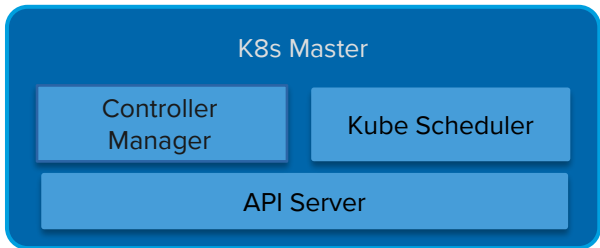
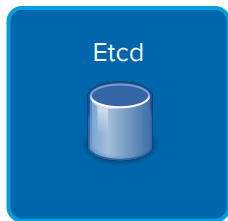
us-tirefire-1c

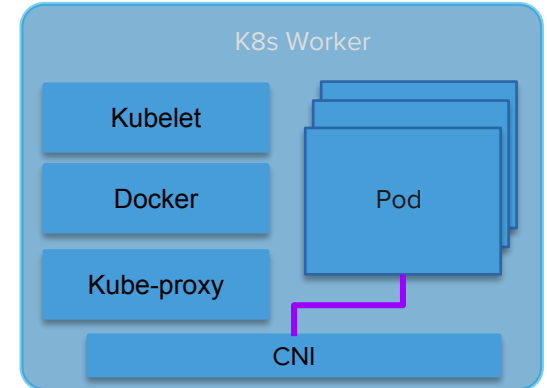
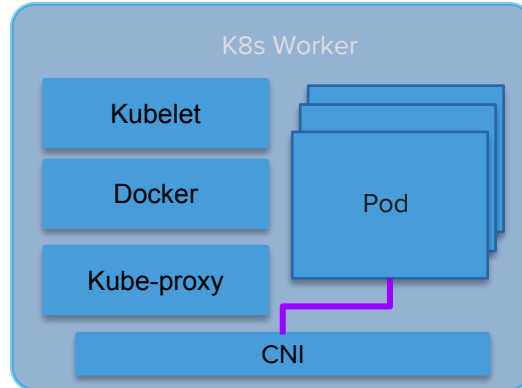
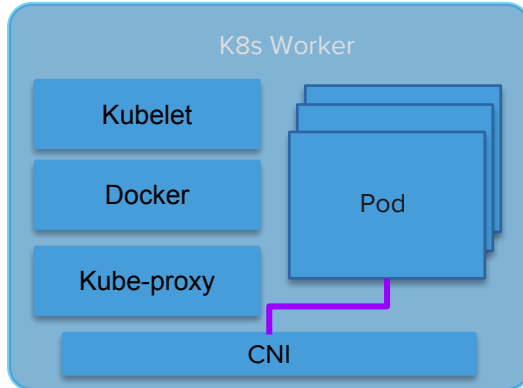
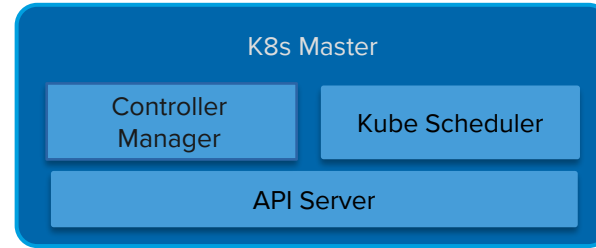
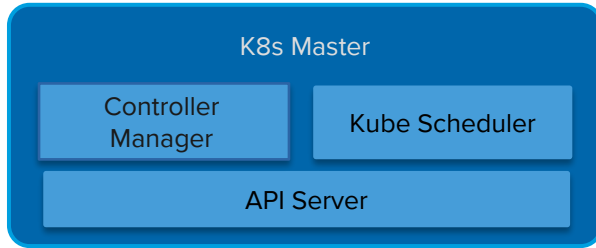
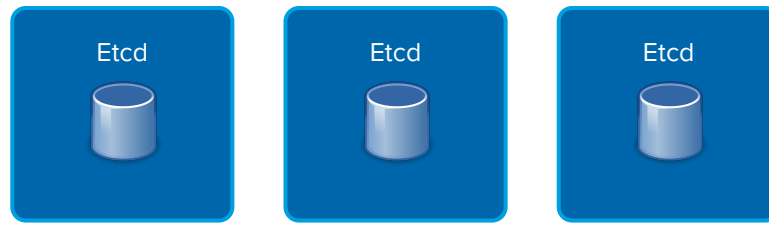


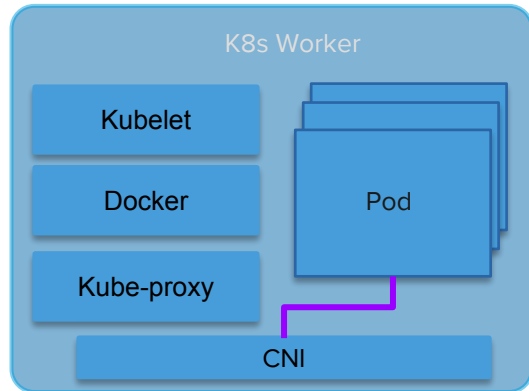
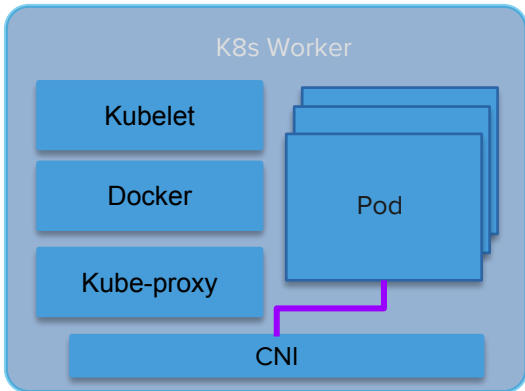
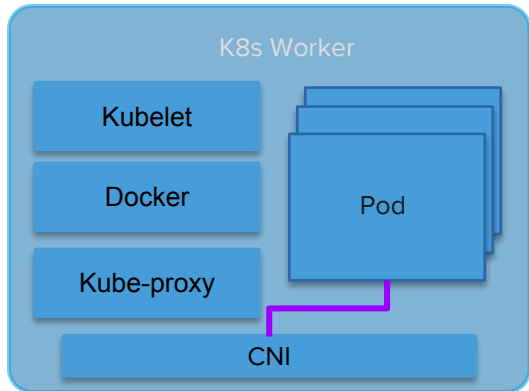
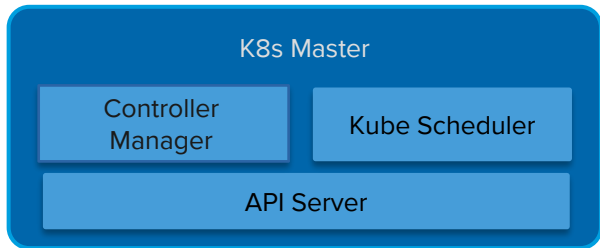
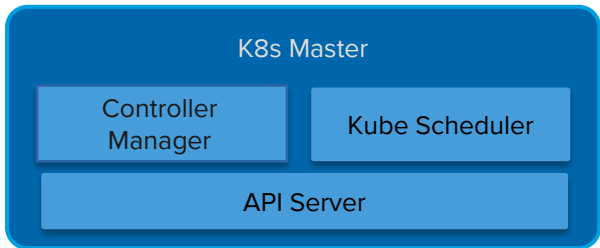
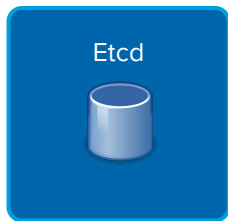
A photograph of two white lambs standing in a lush green field. The lambs are positioned in the center of the frame, with one slightly behind the other. They have white woolly fur and pinkish ears. A semi-transparent yellow horizontal band is overlaid across the middle of the image, containing the text "High Availability" in a black, sans-serif font. The background is a soft-focus green field with some scattered dry leaves.

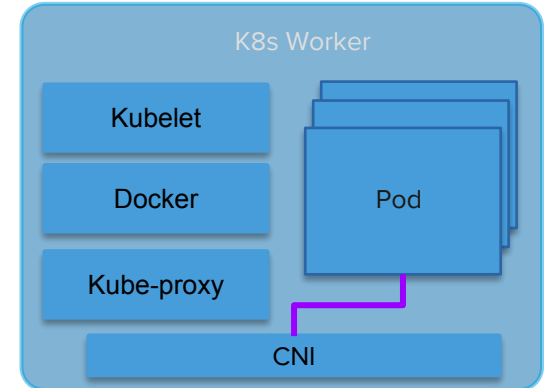
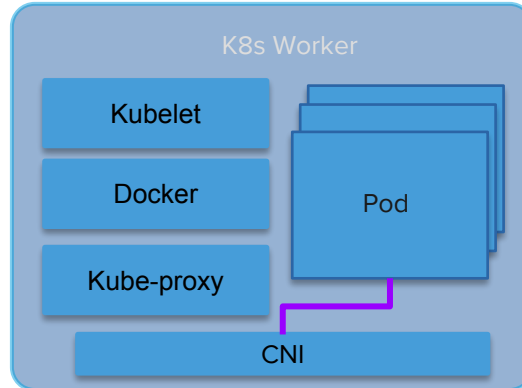
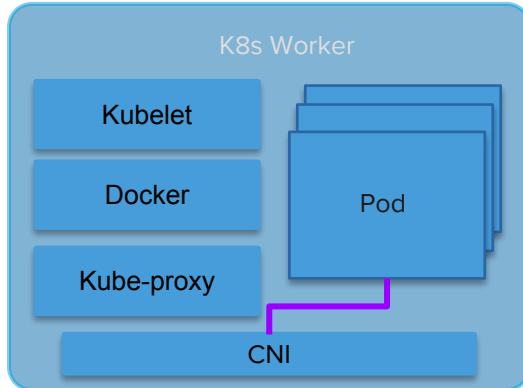
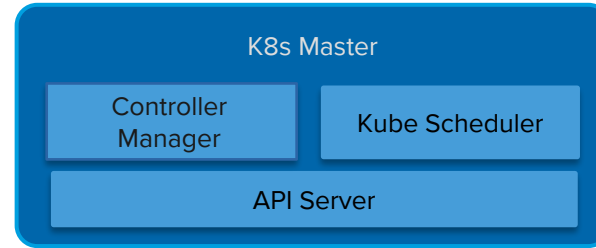
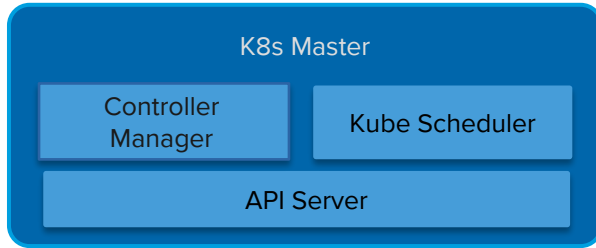
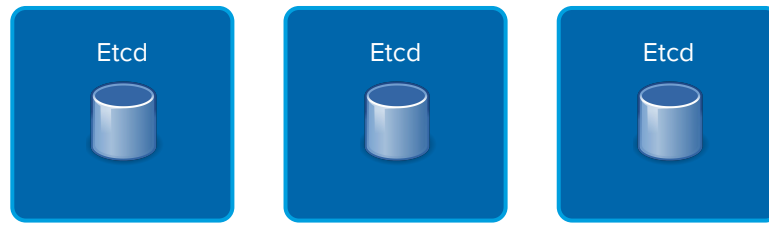
High Availability





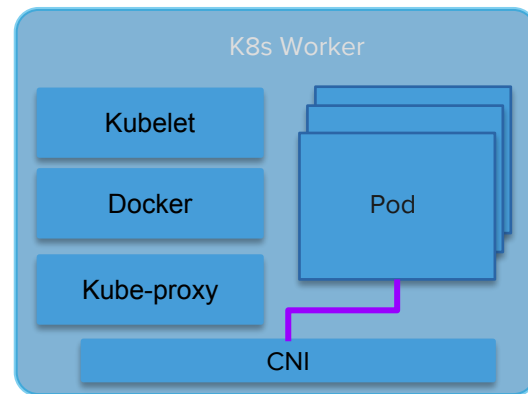
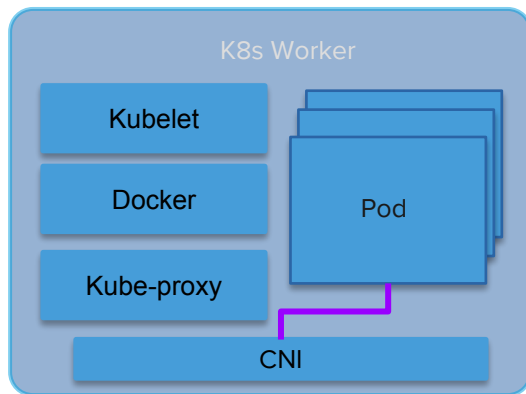
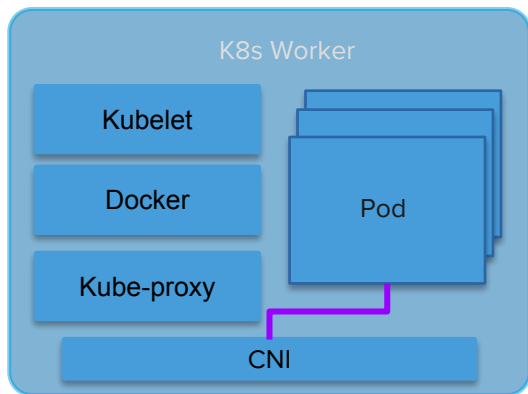
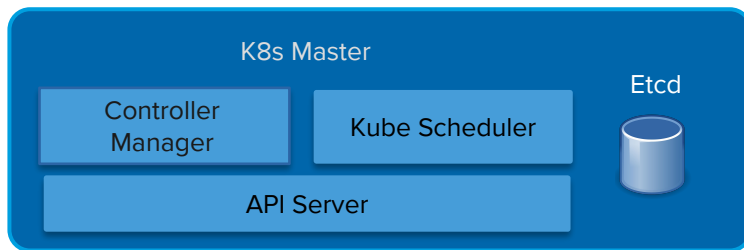








<http://www.bsielearning.com.au/keep-simple-stupid/>



```
5 * @package _$
6 *
7 *
8 */
9
10 if ( ! function_exists( 'incode_starters' ) ) {
11     /**
12      * Sets up theme defaults and registers support for
13      *
14      * Note that this function is hooked into the after_setup_theme
15      * runs before the init hook. The init hook is too late for some features
16      * as indicating support for post thumbnails.
17      */
18     function incode_starters() {
19         // Make theme available for translation
20         // Translations can be filed in the /languages/ directory
21         // If you're building a theme based on incode_starters, you can
22         // change the domain name to the name of your theme. For example,
23         // you could set $domain = 'mytheme' and translate all
24         // strings in your theme with _e( 'string' ) instead of _e( 'string' )
25         //
26         // To change the domain name to the name of your theme,
27         // uncomment the lines below. Don't forget to change the
28         // text domain in the text_domain parameter on the
29         // line 18.
30         //
31         // Text Domain
32         // $domain = 'mytheme';
33         // load_theme_textdomain( $domain, get_template_directory() . '/languages' );
34     }
35 }
```

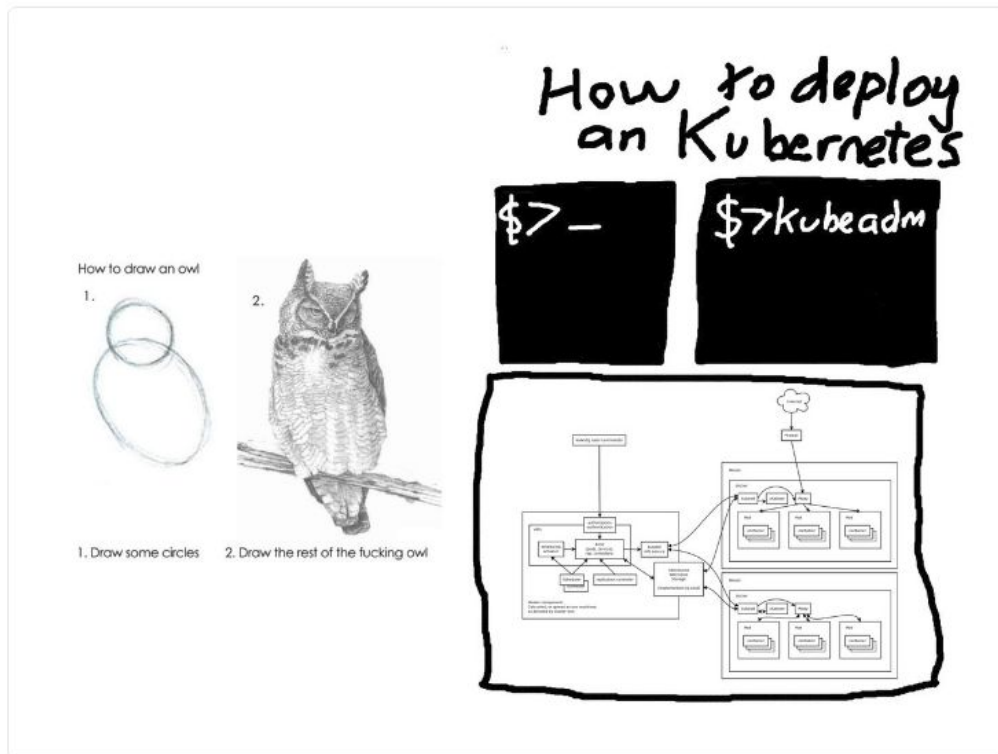
Deployment

Czarcloudski

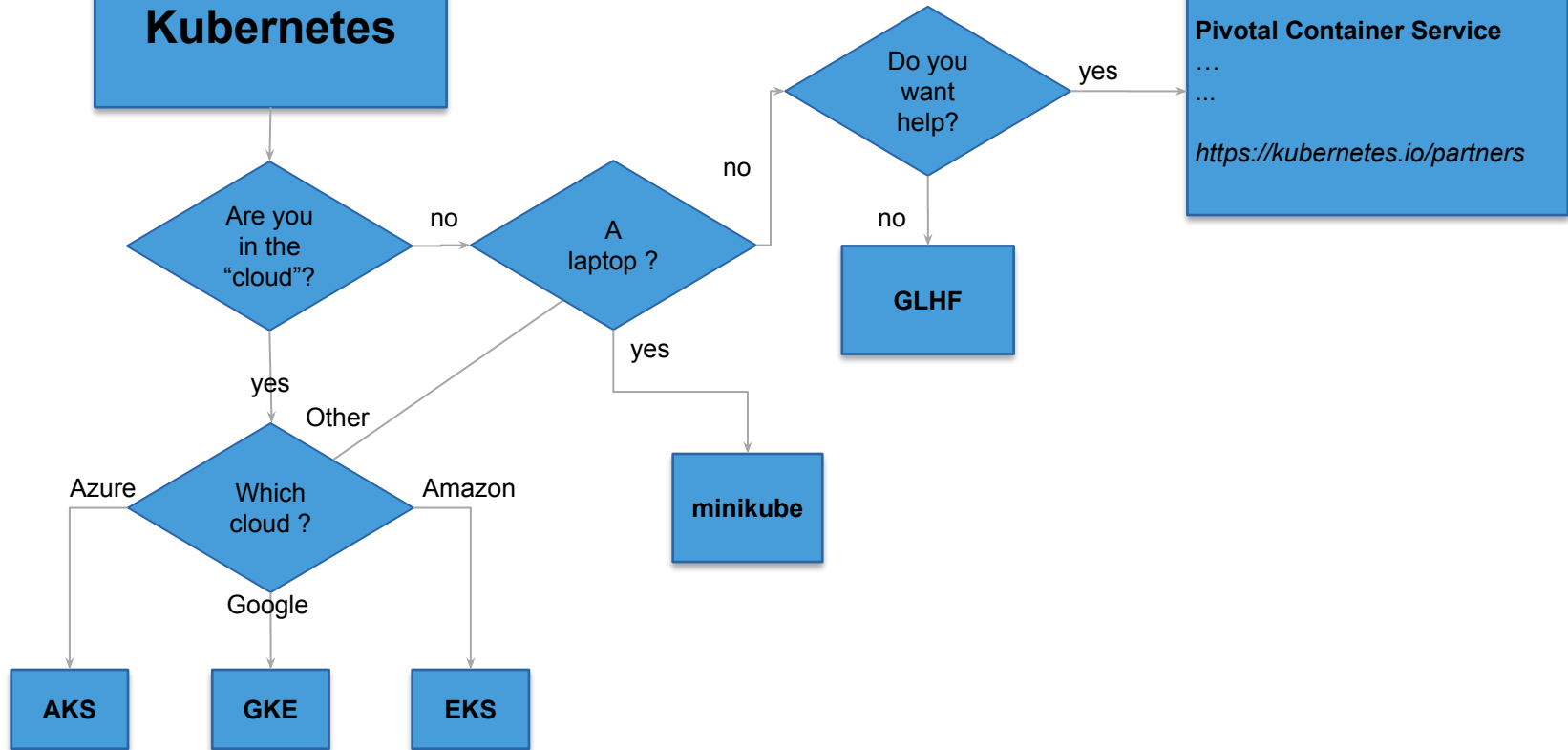
@pczarkowski



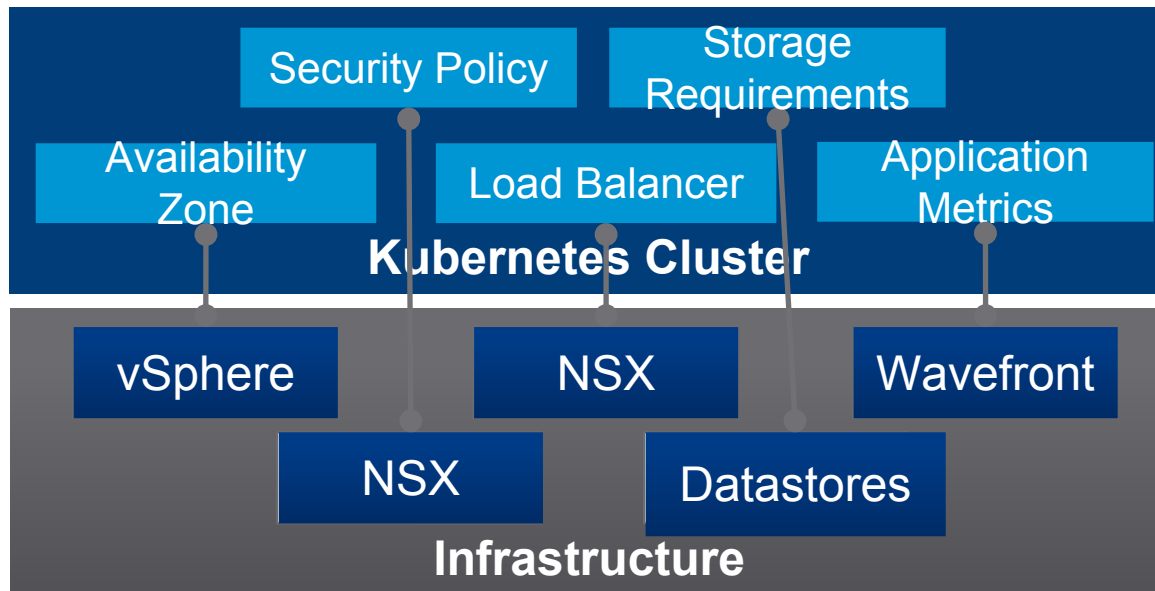
Did you know that Deploying an Kubernetes
is as simple as drawing an Owl ?

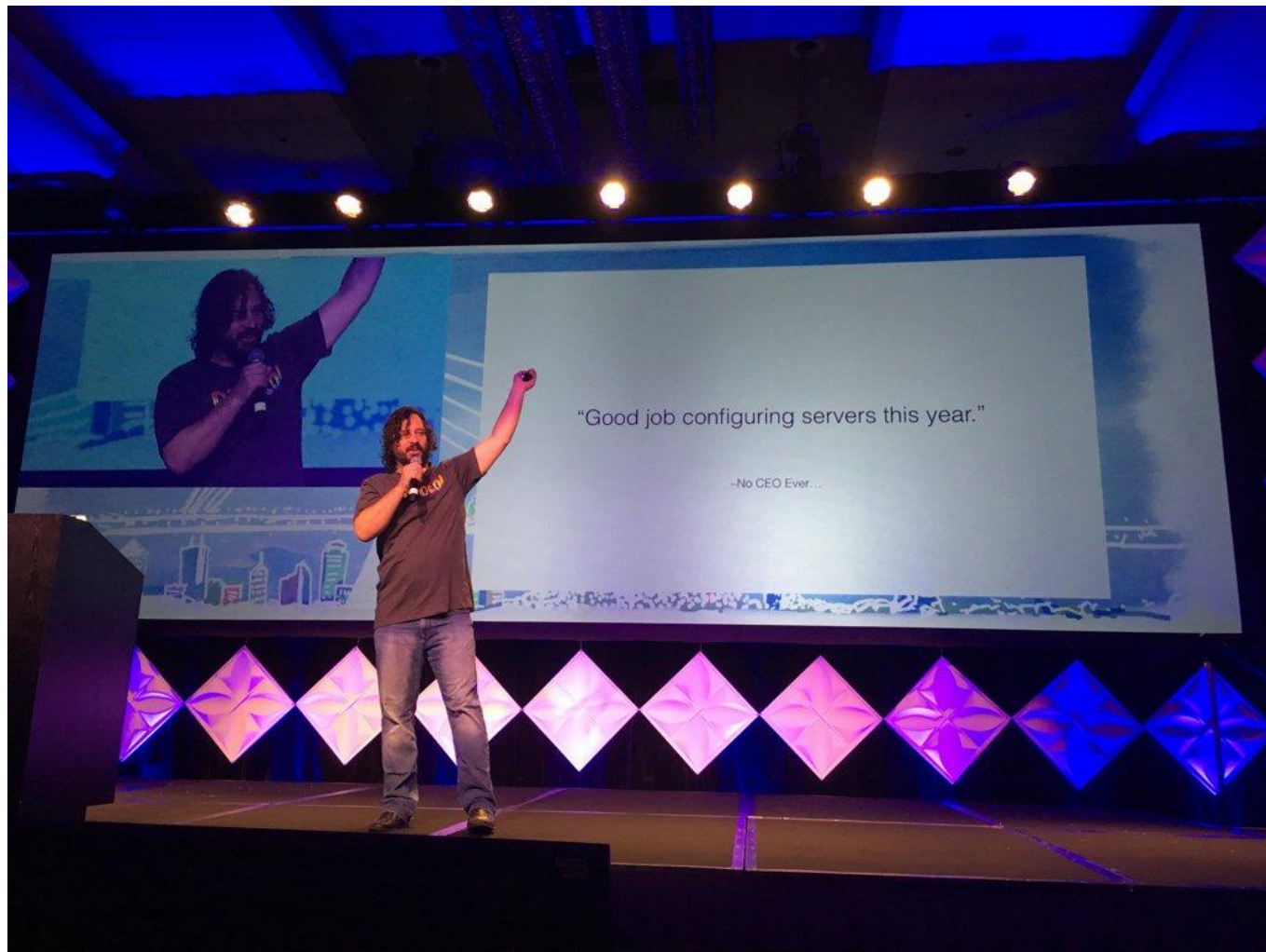


How to Get an Kubernetes



vmware®







Pivotal
Container Service™

<https://docs-cfcr.cfapps.io/>



<https://github.com/kubernetes-incubator/kubespray>



OPENSIFT

<https://github.com/openshift/origin>

Kubespray

<https://github.com/kubernetes-incubator/kubespray>

- Ansible based, so very approachable
- An official Kubernetes (incubator) project
- Good support for CNIs and Cloud Providers
- Combine with one of the Ansible Hardening projects
 - <https://github.com/dev-sec/ansible-os-hardening>
 - <https://github.com/openstack/ansible-hardening>

gitops

- Deployed Platform == code repo + environment repo
 - Ansible - Playbook + Inventory
 - Bosh - Release + Manifest
- Keep it all in git!
 - Fork upstream repo... if only to ensure it doesn't get changed from under you
 - Inventory/Manifest is probably YAML ... perfect to be stored in git.
 - One repo for all envs, or a repo per env ... either is fine.
- Consider using a gitops focussed wrapper around ansible
 - Ursula-cli (<https://github.com/blueboxgroup/ursula-cli>)
 - Gosible (<https://github.com/paulczar/gosible>)
 - Molecule (<https://github.com/metacloud/molecule>)
- Use Jenkins or similar to run tests, deploy test envs, push to prod???
 - But probably not full on Continuous Delivery ... risks are very high!

Validate and Backup

Validate your Kubernetes cluster is conformant!

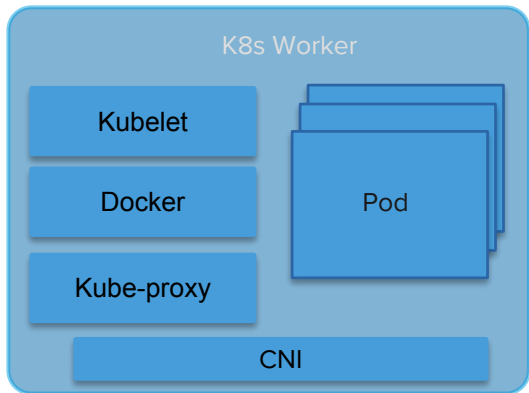
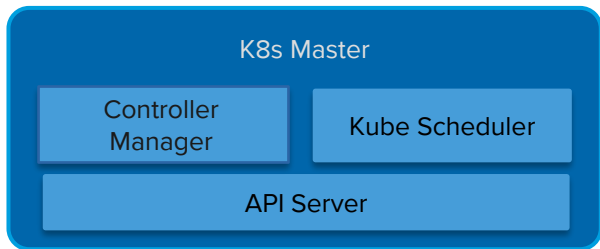
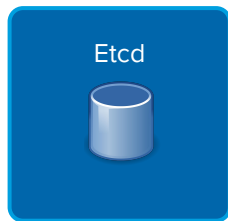
<https://github.com/heptio/sonobuoy>

Backup your Kubernetes cluster state!

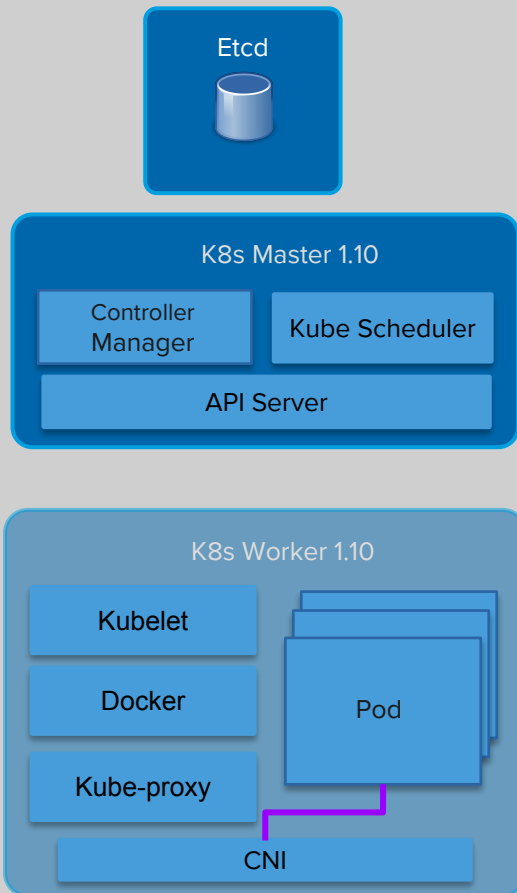
<https://github.com/heptio/ark>

A close-up photograph of a robotic arm, likely a prosthetic or research model, featuring a complex arrangement of metal joints, gears, and numerous thin, white, cable-like structures. The arm is positioned against a bright blue background. In the lower-left foreground, a portion of a white computer keyboard is visible. A semi-transparent orange horizontal band is superimposed across the middle of the image, containing the word "Upgrades" in a black, sans-serif font.

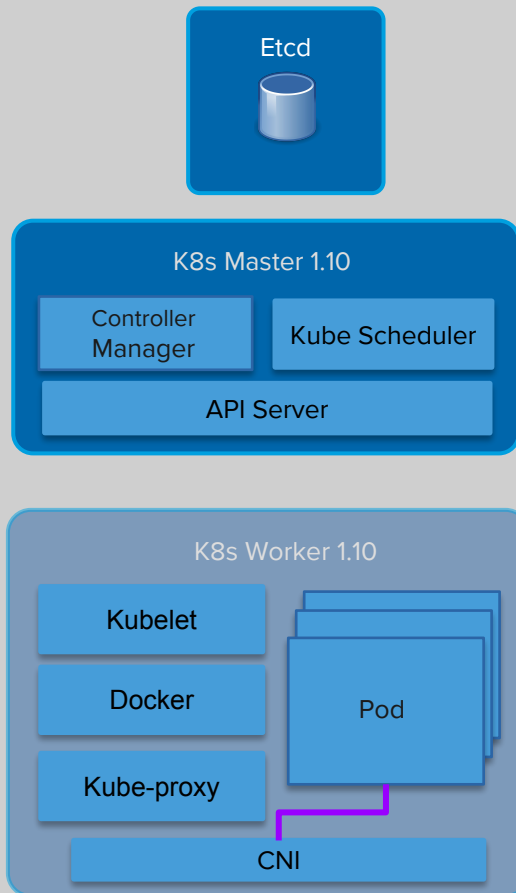
Upgrades



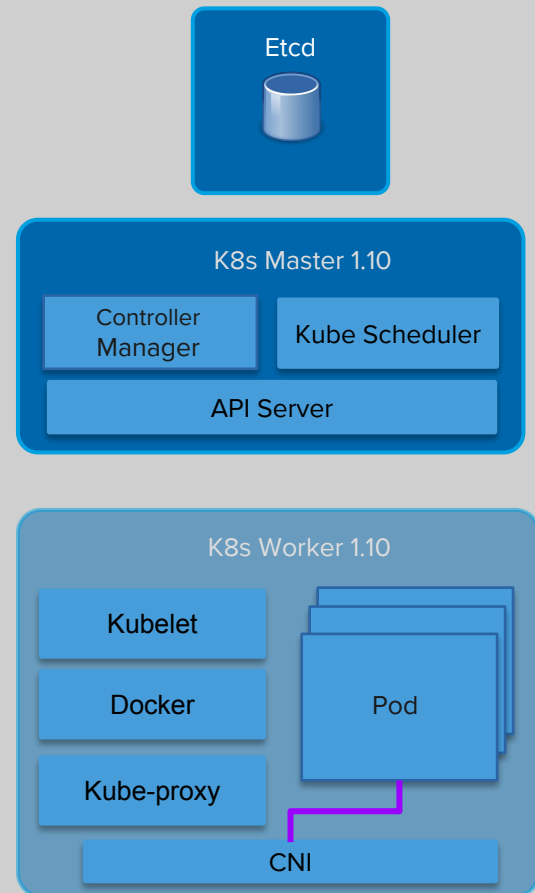
us-tirefire-1a



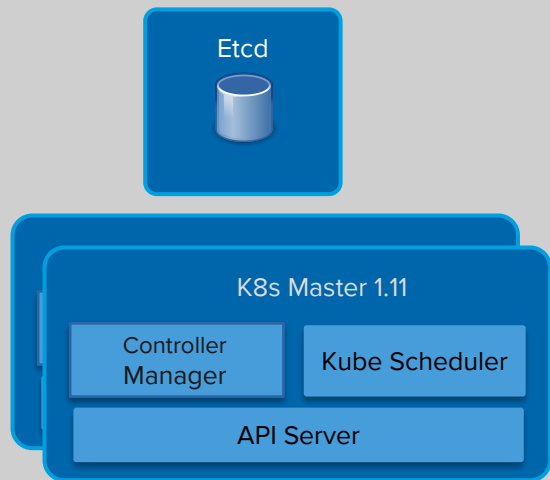
us-tirefire-1b



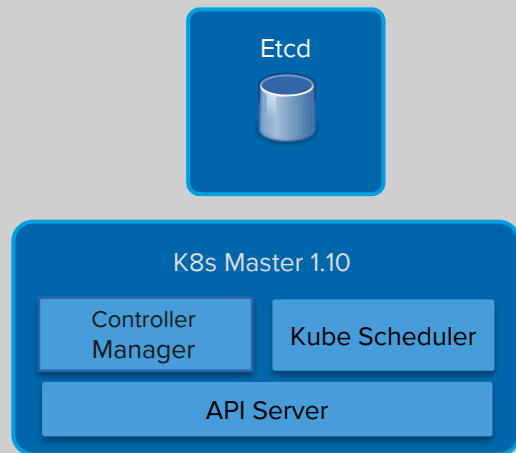
us-tirefire-1c



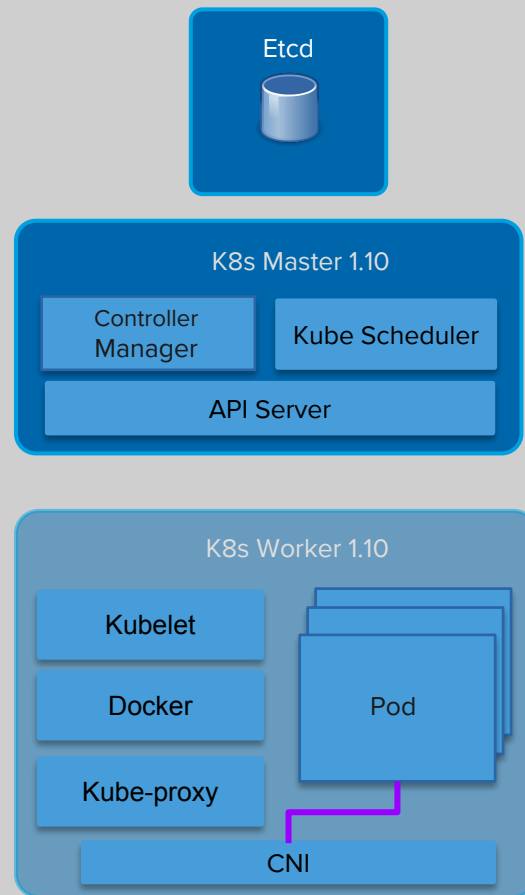
us-tirefire-1a



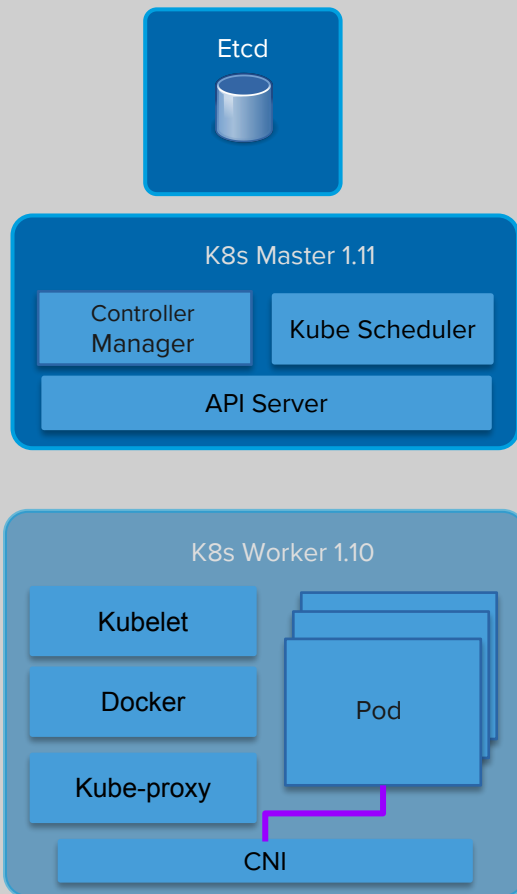
us-tirefire-1b



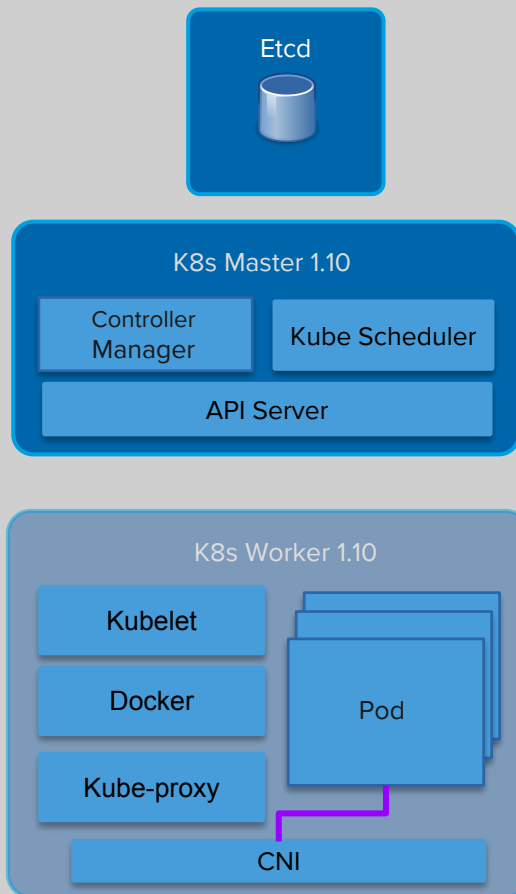
us-tirefire-1c



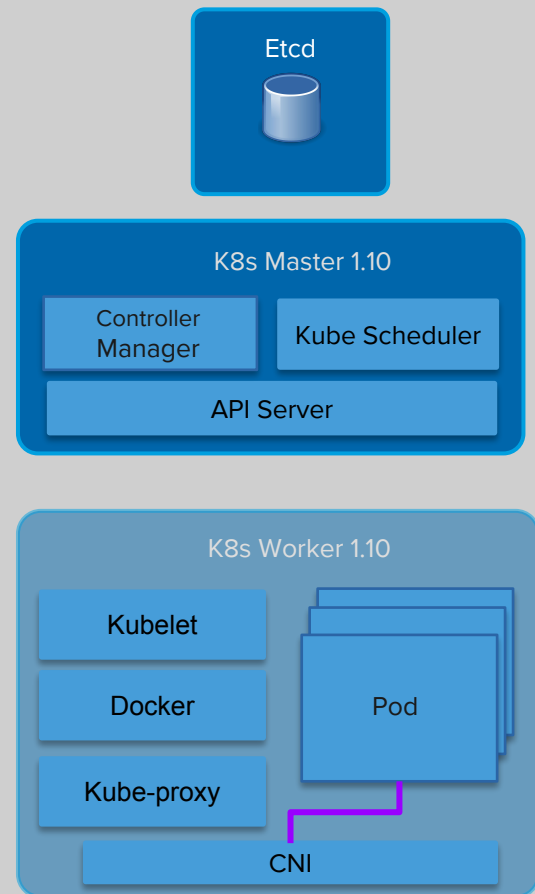
us-tirefire-1a



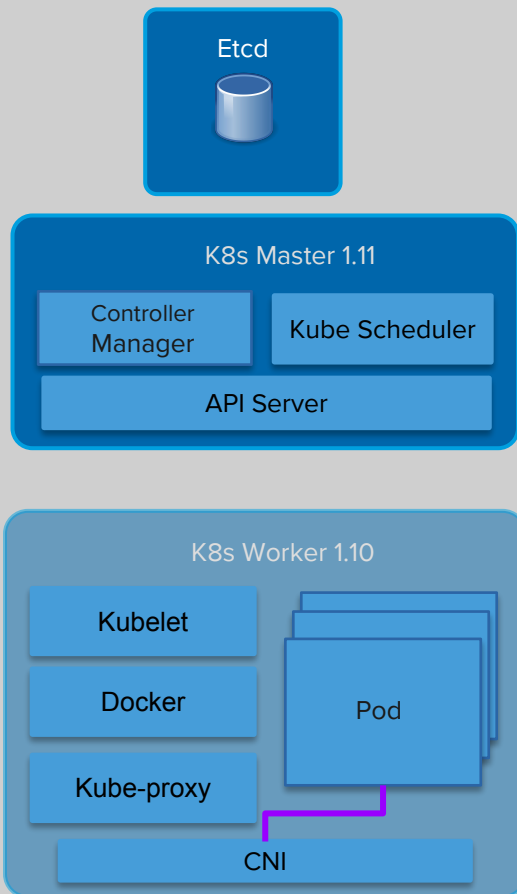
us-tirefire-1b



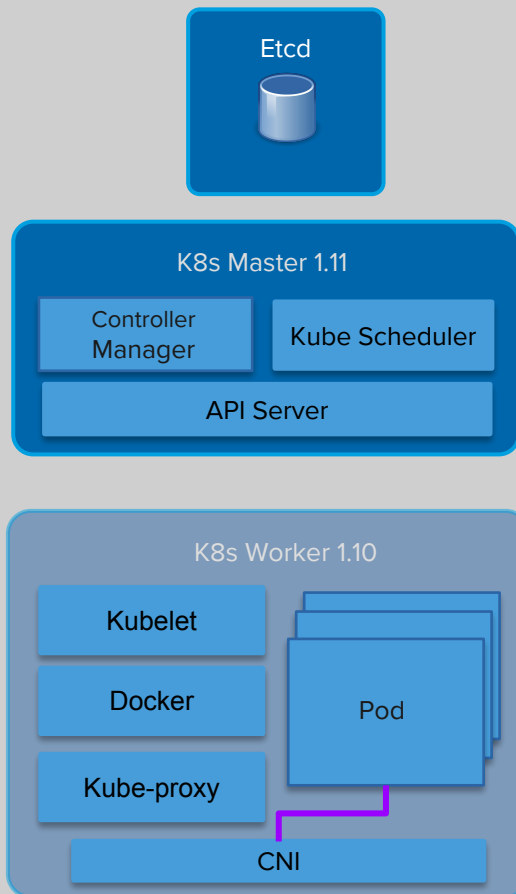
us-tirefire-1c



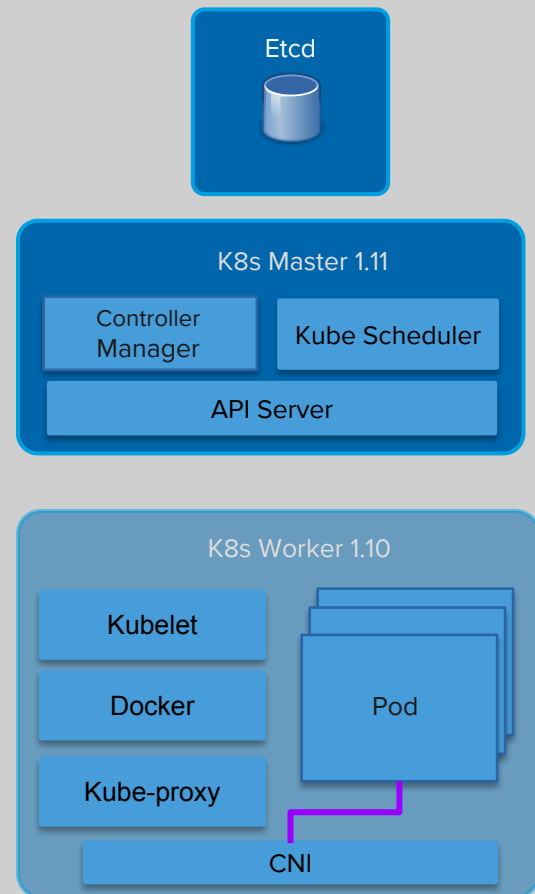
us-tirefire-1a



us-tirefire-1b



us-tirefire-1c



us-tirefire-1a



K8s Master 1.11

Controller
Manager

Kube Scheduler

API Server

K8s Worker 1.11

Kubelet

Docker

Kube-proxy

Pod

CNI

us-tirefire-1b



K8s Master 1.11

Controller
Manager

Kube Scheduler

API Server

K8s Worker 1.10

Kubelet

Docker

Kube-proxy

Pod

CNI

us-tirefire-1c



K8s Master 1.11

Controller
Manager

Kube Scheduler

API Server

K8s Worker 1.10

Kubelet

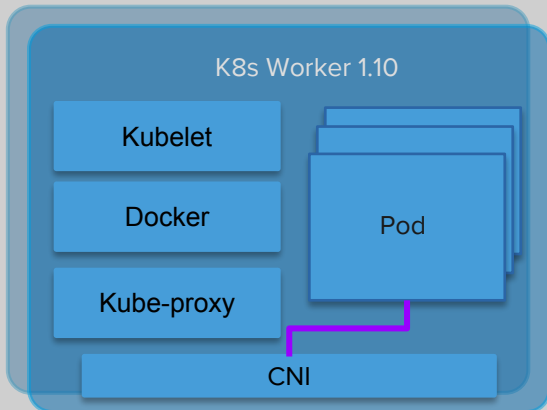
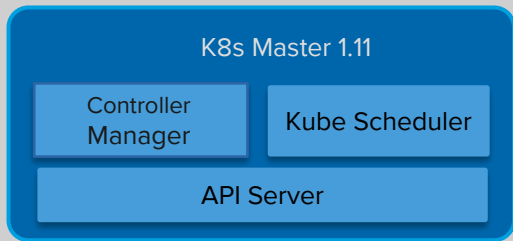
Docker

Kube-proxy

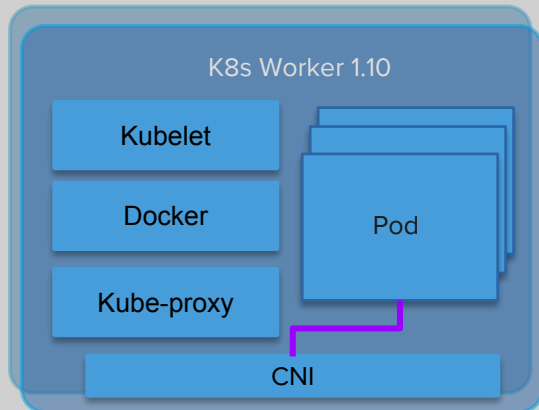
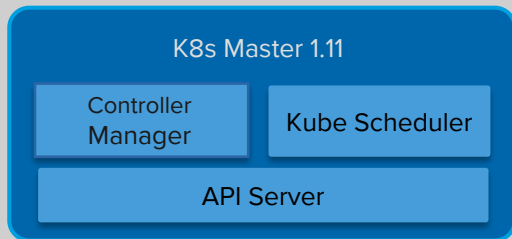
Pod

CNI

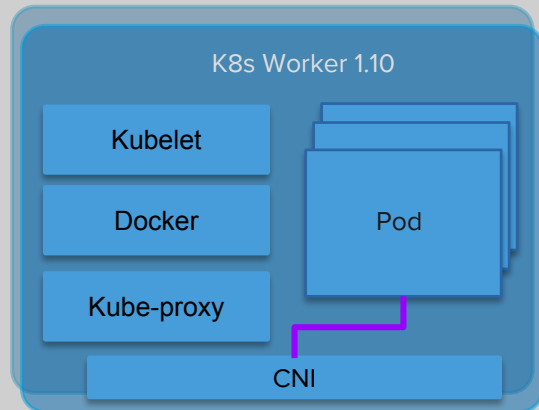
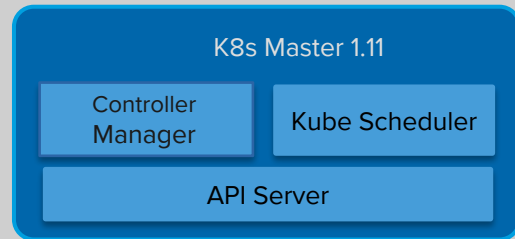
us-tirefire-1a



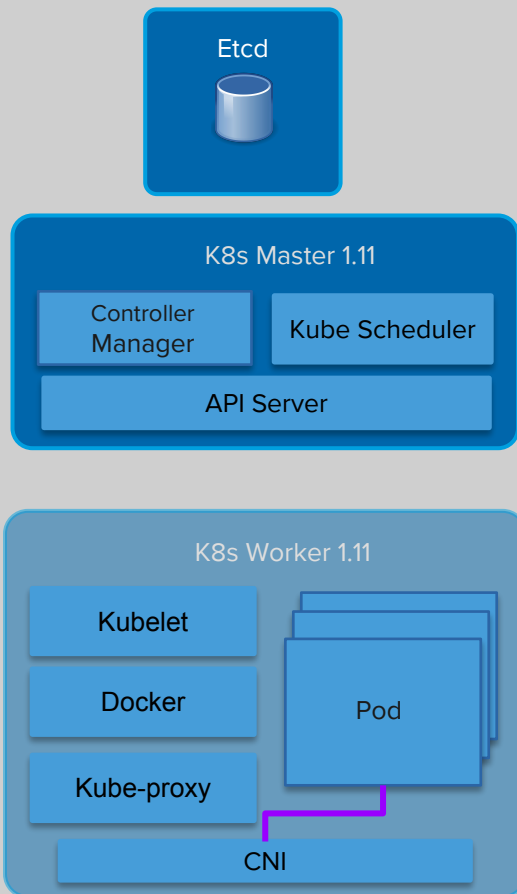
us-tirefire-1b



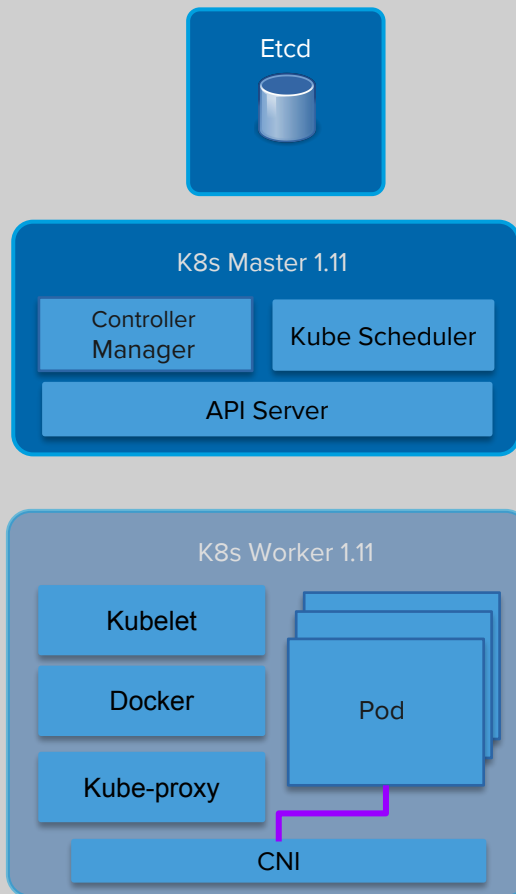
us-tirefire-1c



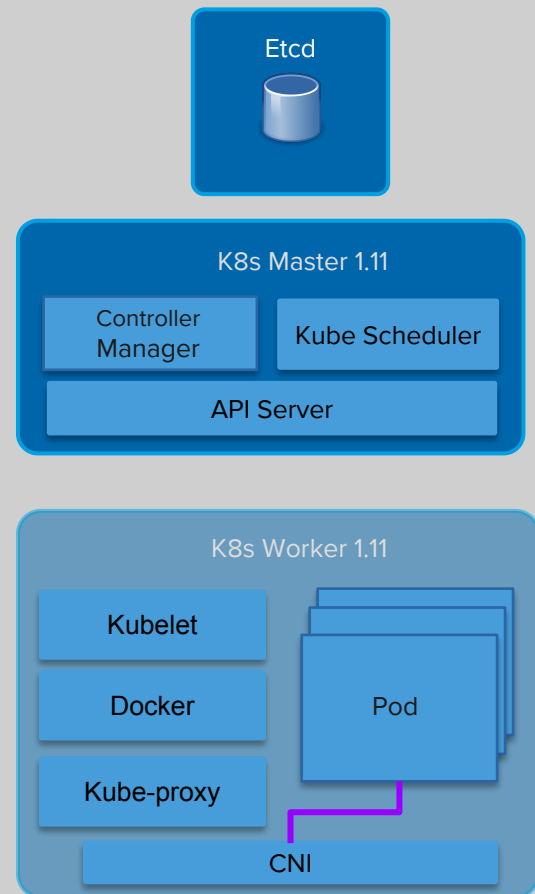
us-tirefire-1a



us-tirefire-1b



us-tirefire-1c





Operations

Monitoring / Logging - The Platform

Server Agents

- Install as binaries / containers on the underlying OS
- No chicken and egg problems
- Extra devops toil (config management etc)
- Direct access to system metrics and logs
- Can use existing tools / processes

Daemonsets

- Run in Kubernetes on each node as daemonset
- If Kubernetes is broken, will the monitoring daemonset be broken ?
- Have to be able to dockerize the agent
- Privileged containers / host volumes to access system metrics and logs
- Masters also have to be workers or can't run daemonset on them.

Monitoring / Logging - Workloads

Kubernetes Metrics API

- Basic point in time pod/node metrics
- `$ kubectl top {node,pod}`
- Adaptors for Prometheus / Graphite / etc

Kubernetes logging

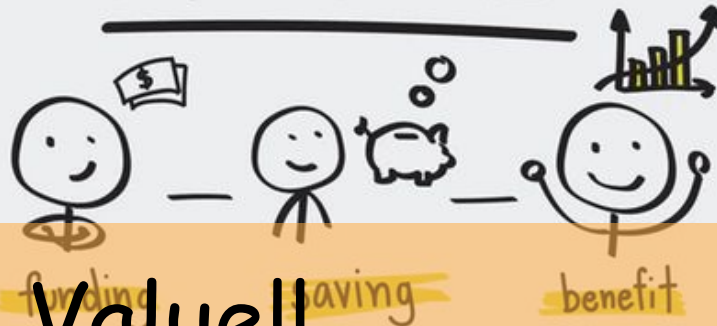
- Kubernetes configures docker to log all Pod stdout/stderr to a file
- `$ kubectl logs <name-of-pod>`
- Need daemonset or agent to read k8s logs from filesystem
- EFK - Elastic, Fluent, Kibana

Authentication / Access Control

- Node vs ~~ABAC~~ vs RBAC
- Service Accounts - managed inside kubernetes
- User Accounts - managed outside kubernetes
 - OpenID Connect
 - Ldap / AD
 - Oauth2
 - Etc
- Secure your Kubernetes Dashboard silly!
 - Everything is TLS encrypted Right ?

```
$ kubectl auth can-i create deployments --namespace dev
yes
$ kubectl auth can-i create deployments --namespace prod
no
```

FINANCE



CASHBOOK

CONTROL AND SAVE YOUR MONEY

Business Company

123 Boulevard de la Paix
Paris 75001
Tel: 01 45 67 89 10
Fax: 01 45 67 89 11

Bill to: Curedur export LTD
456 Palmyresque, Jeddah
21511 Mt. SUD 9999
001-004-321

No.	Description
-----	-------------

Replatforming vs Modernization for PKS

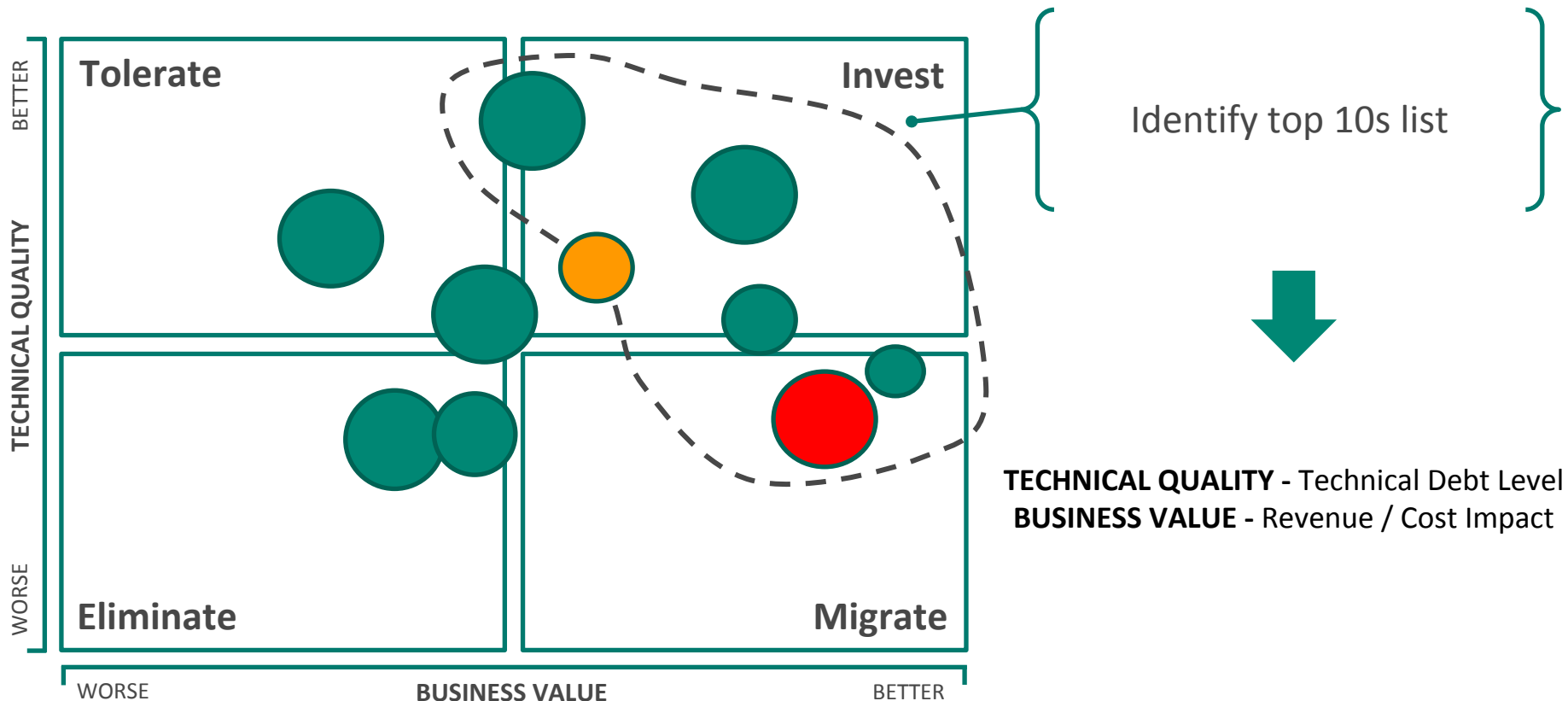
Lift & Shift / Replatforming

- Lift and Shift with “just enough modernization”
- You may not have access to the code
- Revisit decisions made in Greenfield time
 - Around CI/CD process
- Get some quick wins through platform capabilities
 - Reduced operating and infrastructure cost
 - Improved speed to deploy & scale
 - Faster patching of kernel level vulnerabilities

Modernization

- Leverage features in modern cloud platforms
 - Blue/Green deploys
 - Auto-healing
 - Auto-scaling
 - Advanced routing/networking automation
- Design and build based on known Cloud Native patterns
- Longer term investment in the application
- Like you need access to the code
- Plus everything mentioned in “replatforming”

TIME Methodology



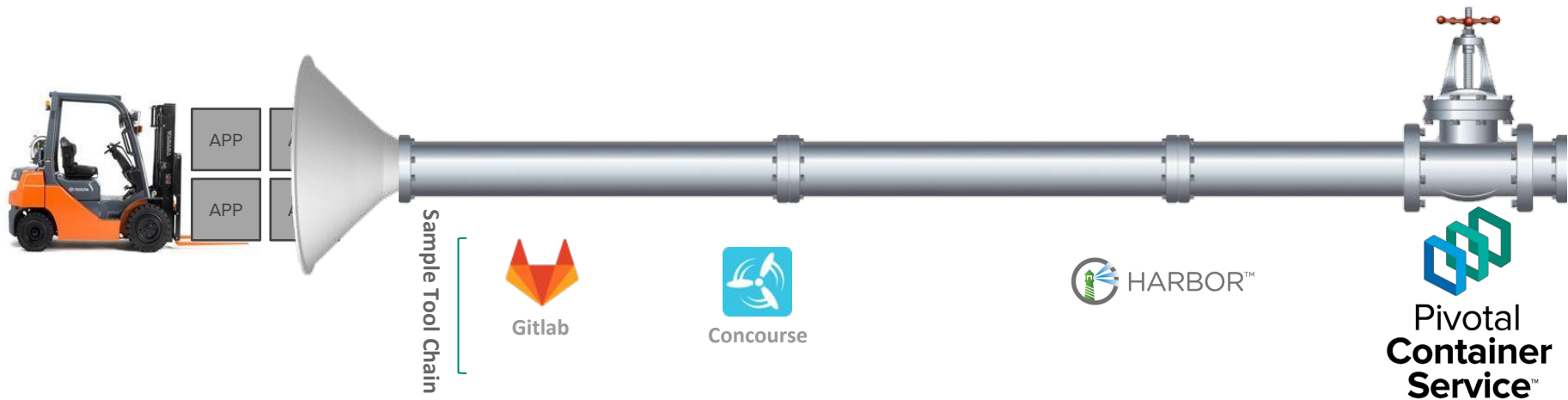
* Gartner's TIME methodology for Application Portfolio Rationalization

1

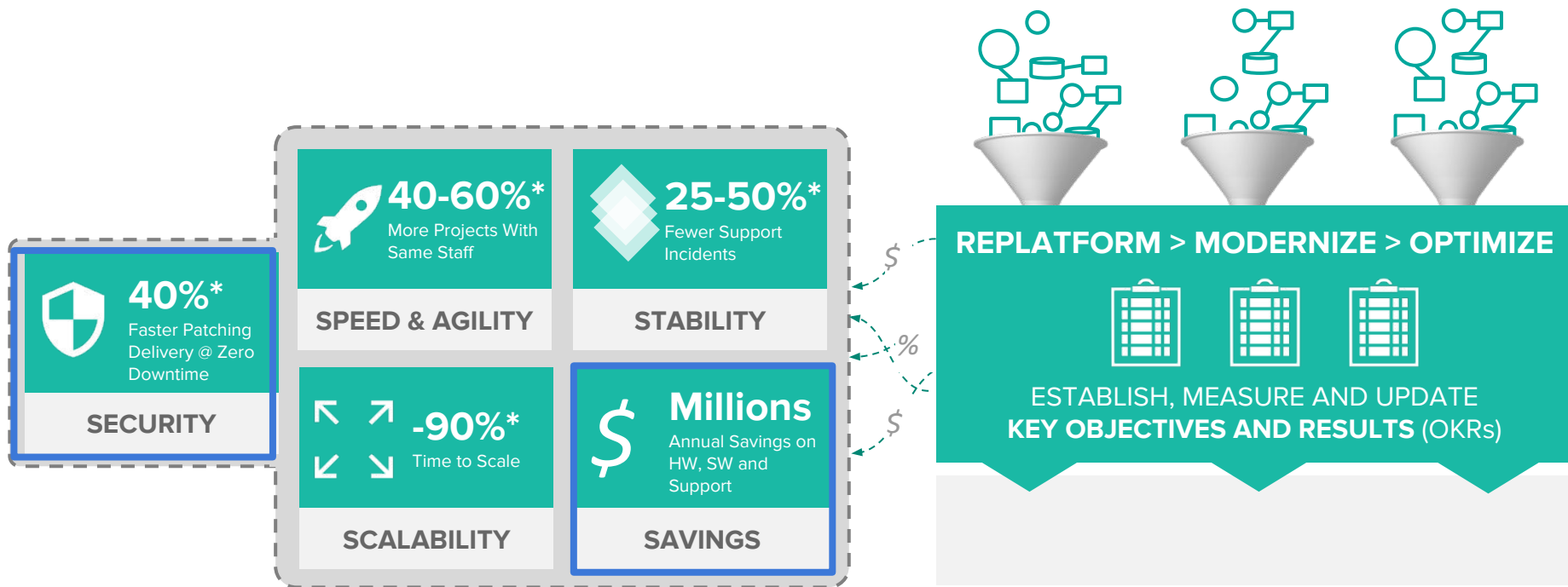
Identify 5-10 apps confirmed as suitable to run on PKS

2

Work on a short project to push a few apps *all the way* to prod and measure the ROI metrics



How We Think about the Business Case



PLATFORM VALUE STREAM AND METRICS



Pivotal®

Transforming How The World Builds Software